State of North Carolina
Office of Information Technology Services

Michael F. Easley, Governor **George Bakolia, State Chief Information Officer**

Memorandum

To: George Bakolia, State Chief Information Officer

From: Ann Garrett, State Chief Information Security Officer

Subject: 2008 Security Standards Review

Date: May 21, 2008

Pursuant to GS 147-33.110, the Enterprise Security and Risk Management Office (ESRMO) performed a security review of the statewide security standards. The following includes the methodology and results of the survey, and subsequent recommendations for the statewide security manual.

Methodology:

ESRMO published and reviewed the survey around three main questions:

- Are there any sections in the security manual that need enhancements or updates?
- Are there any gaps in the security manual for which policies need to be added?
- Are there any standards that the agency owns that would be useful for all state agencies?

A summary document and a spreadsheet with the results from the 2008 Information Security Manual Survey are attached with this memo.

Statewide Information Security Manual Survey Results

The results from the 2008 Statewide Information Security Manual Survey indicate that the current statewide security standards meet the needs of the agencies. ESRMO recommends reviewing and updating as necessary certain standards to improve coverage of some topics, refreshing and reorganizing the appendix 'other' topics and adding some new items to the manual. These recommendations are as follows:

Enhancements to existing standards:

- Review and update wireless network standards (*020117 – Controlled Pathway, 020118 – Node Authentication, 030101 – Configuring Networks, 090301 – Electronic Eavesdropping*)

P.O. Box 17209 • Raleigh, North Carolina 27619-7209
Tel: 919.981.5555 • Fax: 919.981.2548 • State Courier 51-01-11

- Review and update encryption standards (*030203 – Controlling Data Distribution and Transmission, 030205 – Managing Electronic Keys, 030801 – Using Encryption Techniques*)
- Review and update business continuity management standards (*Chapter 14 Planning for Business Continuity and* (*Chapter 3, Section 06 – Backup, Recovery and Archiving*)
- Review and update section on Backing Up Data on Portable Computer (*Chapter 3, Section 030602*)
- Review and update as necessary the 'Other Security Standards and Policies'. Incorporate these other topics into the manual chapters whenever possible. (**Bold** indicates a priority item)
    - Application Security Policy with Guidelines
    - Confidential Security Information Policy
    - **Desktop and Laptop Security Standard**
    - DNS Enterprise Security Standard
    - **Electronic Mail Server Security Standard**
    - Enterprise Authentication and Authorization Services Policy
    - Firewall Configuration Security Standard
    - Identification and Authentication Using IDs and Passwords
    - **Information Technology Risk Management Policy with Guidelines**
    - **Public Key Infrastructure and Digital Certificates – Intranet**
    - **Remote Access Security Standard**
    - User Id and Password Protection Standard

New items

- Add guidance on security for virtual machines
- Include a definition for a 'personal computing device'

If you have any questions concerning this review, please contact Ann.Garrett@its.nc.gov or 919-981-5130.

cc: Sharon Hayes, Deputy State Chief Information Officer
Bill Willis, Deputy State Chief Information Officer
Danny Lineberry, Senior Advisor for IT Programs

Attachments: 2008 Security Standards Survey Results.xls
2008 Survey Analysis.doc